VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Absolvování individuální odborné praxe

Individual Professional Practice in the Company

2016 Šimon Pánik

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Zadání bakalářské práce

Student: **Šimon Pánik**

Studijní program: B2647 Informační a komunikační technologie

Studijní obor: 2612R025 Informatika a výpočetní technika

Téma: Absolvování individuální odborné praxe
Individual Professional Practice in the Company

Jazyk vypracování: čeština

Zásady pro vypracování:

1. Student vykoná individuální praxi ve firmě: Tieto Czech s.r.o.
2. Struktura závěrečné zprávy:
   a) Popis odborného zaměření firmy, u které student vykonal odbornou praxi a popis pracovního zařazení studenta.
   b) Seznam úkolů zadaných studentovi v průběhu odborné praxe s vyjádřením jejich časové náročnosti.
   c) Zvolený postup řešení zadaných úkolů.
   d) Teoretické a praktické znalosti a dovednosti získané v průběhu studia uplatněné studentem v průběhu odborné praxe.
   e) Znalosti či dovednosti scházející studentovi v průběhu odborné praxe.
   f) Dosažené výsledky v průběhu odborné praxe a její celkové zhodnocení.

Seznam doporučené odborné literatury:

Podle pokynů konzultanta, který vede odbornou praxi studenta.

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **doc. RNDr. Petr Šaloun, Ph.D.**

Konzultant bakalářské práce: Ing. Richard Biječek

Datum zadání: 01.09.2015

Datum odevzdání: 29.04.2016

doc. Dr. Ing. Eduard Sojka
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě 29. dubna 2016 .....

Souhlasím se zveřejněním této bakalářské práce dle požadavků čl. 26, odst. 9 Studijního a zkušebního řádu pro studium v bakalářských programech VŠB-TU Ostrava.

Tieto Czech s.r.o.
28. října 3346/91
702 00 Ostrava - Moravská Ostrava
IČO 64608051 DIČ CZ64608051

V Ostravě 27. dubna 2016

.....
JIRÍ FRANZ

Rád bych na tomto místě poděkoval Ing. Richardovi Biječkovi, za cenné rady a doporučení pro psaní této práce, mým kolegům, především Janovi, za konzultace při řešení komplikovaných úloh, a také svému vedoucímu práce, doc. RNDr. Petru Šalounovi, Ph.D. za vedení bakalářské práce.

Abstrakt

Tato bakalářská práce se zabývá mým absolvováním odborné praxe ve společnosti Tieto Czech na pozici Windows Server Administrator. Práce je rozdělena na teoretickou a praktickou část. První část je věnována informacím o společnosti a pozici, na které jsem praxi vykonal. Dále se zabývá procesy ITIL, kterých bylo nutné se při vykonávání praxe držet a stručně charakterizuje technické prostředí. Druhá část práce je zaměřena na charakteristiku konkrétních úloh, které jsem během své praxe vykonával. Dále obsahuje vyhodnocení mých dosažených výsledků a zkušeností získaných během praxe.

Klíčová slova: ITIL, Tieto, praxe, Microsoft Windows, server, technická podpora, správa systému

Abstract

This bachelor thesis deals with completing my professional practice in the Company Tieto Czech on position Windows Server Administrator. The thesis is divided into theoretical and practical part. The first part is devoted to information about the company and the position on which I did my practice. It also deals with the ITIL processes which were necessary to follow during my practice and briefly describes the technical environment. The second part focuses on the characteristics of the specific tasks that I performed during my practice. It also includes an evaluation of my achievements and experiences gained during practice.

Key Words: ITIL, Tieto, practice, Microsoft Windows, server, technical support, system administration

Obsah

Seznam použitých zkratek a symbolů

CI	–	Configuration Item
CIFS	–	Common Internet File System
CM	–	Configuration Management
CMDB	–	Configuration Management Database
DHCP	–	Dynamic Host Configuration Protocol
DNS	–	Domain Name System
ID	–	Identifikátor
IIS	–	Internet Information Services
IP	–	Internet Protocol
IT	–	Informační technologie
ITIL	–	Information Technology Infrastructure Library
KEDB	–	Known Error Database
MS SQL	–	Microsoft SQL Server
NAS	–	Network-attached storage
NSH	–	Network Shell
OLA	–	Operational Level agreement
OS	–	Operační systém
SAN	–	Storage area network
SLA	–	Service Level Agreement
TCP/IP	–	Transmission Control Protocol/Internet Protocol

1 Úvod

Možnost absolvovat odbornou praxi místo bakalářské práce mě zaujala již v prvním ročníku, a to hlavně z důvodu možnosti aplikovat své znalosti v praxi a získat další cenné zkušenosti. Praxi na pozici Windows Administrator jsem si vybral z důvodu mého blízkého vztahu ke správě systémů, především tedy Windows systémů, a navazovala na mé předešlé znalosti a zkušenosti se správou stanic. Využil jsem tedy této možnosti rozšířit si znalosti v oblasti správy serverů. Ačkoliv technické znalosti pro správu jednotlivých typů systému jsou odlišné, obecné postupy, jako jsou procesy ITIL a zásady pro vzdálenou správu, jsou velice podobné i pro Unixové operační systémy. V této práci se postupně zabývám potřebnými teoretickými znalostmi k vykonávání práce na této pozici, a to hlavně z pohledu procesů, se kterými jsem se musel seznámit a dodržovat je během technických zásahů. Dále stručně popisuji technické prostředí, ve kterém jsem pracoval. V druhé kapitole se poté zabývám okruhy témat, které jsem během své praxe řešil a celkovým hodnocením této praxe.

2 Teoretická část

2.1 O společnosti Tieto

Společnost Tieto Corporation je největším severoevropským dodavatelem IT služeb, poskytující služby pro soukromý i veřejný sektor po celém světě, především pro středně velké a velké organizace. Společnost sídlí v Helsinkách a celkem zaměstnává více než 15 000 expertů. K nejvýznamnějším zákazníkům společnosti patří Nokia, RWE, Nordea Bank, Stora Enso a další.

Společnost byla založena v roce 1968 ve finském Espoo pod názvem Tietotehdas Oy. Jejím zaměřením bylo poskytovat IT služby pro finské banky a lesní průmysl. V 70. letech poté vzrostlo množství zákazníků a společnost se zaměřila na osobní počítače a vývoj softwaru. V 90. letech došlo k velkému rozvoji společnosti díky uzavírání nových kontraktů. V roce 1995 se společnost přejmenovala na TT Tieto a v roce 1998 na Tieto. Od roku 1999 nesla společnost název TietoEnator, po fúzi se švédskou společností Enator. V roce 2009 došlo ke změně organizační struktury, kdy se společnost začala znovu soustředit na severský trh a začala používat název Tieto Corporation.

Do České republiky vstoupila společnost v roce 2001 a v roce 2004 otevřela své softwarové centrum v Ostravě. Na konci roku 2012 bylo v Ostravě otevřeno nové sídlo Tieto Towers, kde byli přestěhováni zaměstnanci z několika různých budov. Nyní je společnost se svými více než 2 000 zaměstnanci třetí největší pobočkou společnosti Tieto a jedním z největších IT zaměstnavatelů v České republice. Ostravská pobočka poskytuje kompletní IT řešení pro významné zákazníky společnosti, mezi které patří finské vládní organizace, územní samosprávní celky ve Švédsku, finanční společnosti, ocelářský a dřevozpracující průmysl, telekomunikační společnosti a další. Pro tyto zákazníky poskytuje kompletní IT řešení, vývoj softwaru, správu infrastruktury, poradenství a řešení v oblasti IT. [1, 2]

2.2 Popis pracovní pozice

Praxi ve firmě jsem absolvoval na pozici Windows Server Administrator na úrovni 2. stupně technické podpory podle ITIL rozdělení. Specialista na této pozici má za úkol řešení náročnějších událostí, které nemohou být vyřešeny na úrovni zákaznické podpory, případně se jedná o samotnou údržbu infrastruktury. Náplní práce je především technická podpora pro zajištění nepřetržitého provozu služeb, řešení Incidentů a jejich následků, kompletní správa operačního systému Windows Server, zajištění výměny hardwaru v kooperaci s On-Site podporou od dodavatele, zpracovávání zákaznických požadavků a případná pomoc ostatním týmům při řešení aplikačních potíží. Požadována je dobrá znalost operačního systému Windows Server a jeho služeb, orientace v hardwaru, základní znalost sítí a protokolů TCP/IP, služeb DHCP a DNS a znalost virtualizačních technologií Hyper-V a VMware.

2.3 Procesní stránka

Aby bylo možné zajistit služby určité kvality, je potřeba držet se předem stanovených pravidel a postupů – procesů. Společnost Tieto vychází z pravidel ITIL, což je soubor doporučení pro společnosti poskytující IT služby, popisující obecné procesy, které umožňují efektivnější organizaci práce s důrazem na kvalitu poskytovaných služeb. Tyto postupy byly přizpůsobeny interní politice a jsou nazývány jako Tieto Way. Od každého zaměstnance je vyžadováno, aby byl s procesy, které souvisejí s výkonem jeho práce, dobře seznámen a postupoval podle nich. Procesy a způsob práce jsou svázány s informačním systémem, který společnost využívá. Zde je využíván systém TONE, který je založen na řešení od společnosti ServiceNow. Jedná se o běžný tiketovací systém, který umožňuje vést evidenci všech požadavků a událostí ve formě tiketu. Ten je poté přidělen specialistovi, který zajistí jeho další řešení. Systém má také další využití, jako např. CMDB nebo KEDB.

2.3.1 Configuration Management

Smyslem procesu Configuration Management je vést databázi všech elementárních položek, ke kterým se vztahuje poskytovaná služba. Každá tato položka je nazývána CI a je uchovávána v databázi CMDB. V praxi se jedná např. o hardwarový nebo virtuální server, switch, router, síťové úložiště dat (NAS, SAN), může se ale také jednat o samotnou aplikaci běžící na serveru, např. instance MS SQL databáze, webové stránky aj. CMDB poté reprezentuje zjednodušený konceptuální model infrastruktury a služeb, které jsou poskytovány. To nám umožňuje vidět propojení mezi jednotlivými komponentami a rychle určit např. možné následky při výpadku jednoho serveru apod. Propojení klíčových komponent patří mezi hlavní požadavky CM, dále sem patří kvalita dat a jejich pravidelná údržba. [6]

2.3.2 Event Management

Účelem Event Management procesu je generovat a detekovat oznámení o stavu IT infrastruktury a služeb. Pod pojmem Event si můžeme představit výskyt každé události, kterou jsme schopni detekovat, jenž může negativně ovlivnit dodání IT služeb dle dohodnutých podmínek se zákazníkem. Event může být vygenerován monitorovacím nástrojem, nebo samotným CI. Může se tedy projevit jako výskyt chybové zprávy v logu, pád aplikace, nedostupnost serveru, selhání hardwaru aj. Pro Event, který nevyžaduje dalšího zpracování, se využívá tzv. filtrování. V praxi se jedná o zdokumentované případy, kdy Event nemá vliv na poskytovanou službu a nevyžaduje dalšího přezkoumání. Příkladem může být výskyt konkrétní chybové zprávy v systémovém logu.

V případě plánované změny stavu služby se využívá tzv. monitoring supress. Jeho účelem je zabránit generování zbytečných Eventů, které jsou způsobeny plánovanou údržbou, např. patchováním. Příklad si můžeme ukázat na plánovaném restartování serveru. Ten by za běžných okolností vyvolal Event o nedostupnosti serveru a další Eventy při spuštění monitorovacího nástroje, který by detektoval v té době ještě nespuštěné služby a zprávy ze systémového logu, které

se mohou v případě restartování vygenerovat. Monitoring supress pomáhá tomuto předcházet takovým způsobem, že všechny Eventy zadržuje po předem stanovenou dobu. Během této doby čeká na tzv. clearing message, což je Event, který oznamuje informaci o nápravě do korektního stavu (např. server je již znovu dostupný). Po skončení stanoveného intervalu dochází ke kontrole, zda je tento Event stále aktuální a zda má být dále zpracováván. Alternativou je poté monitoring blackout, kdy po stanovenou dobu dochází k zahození všech generovaných Eventů.

Každý Event, který není ovlivněn pravidly pro filtrování a monitoring supress, je zaznamenán ve formě tiketu, jehož zpracování se řídí procesem Incident Management. Tiket je doplněn o další informace ze CMDB, např. zdroj Eventu, tedy CI, priorita, název zákazníka, typ poskytované služby a další informace, které usnadňují jeho řešení. Taktéž jsme schopni zobrazit všechny ostatní Incidenty ze stejného CI a zjistit možné související problémy. [7]

2.3.3 Incident Management

Proces Incident Management popisuje aktivity spojené s obnovením poskytovaných služeb při jejich neplánovaném přerušení, nebo snížení jejich kvality. Na rozdíl od Problem Managementu není primárním účelem nalézt zdroj problému, ale obnovit službu do původního (korektního) stavu v co nejkratším čase. Incident může vzniknout na základě události z Event Managementu, tedy např. z monitorovacího nástroje nebo na základě kontaktování technické podpory zákazníkem. Samotný tiket poté slouží jako dokumentace o průběhu řešení konkrétního výskytu události na konkrétním CI nebo službě.

Priorita řešení Incidentů vychází ze SLA, což je smlouva mezi poskytovatelem IT služeb a zákazníkem, která mimo jiné definuje dobu, za jakou bude v případě výskytu Incidentu služba obnovena. Jsou definovány dvě časové hodnoty, které se označují jako *Responce time* a *Resolution time*. První hodnota nám udává dobu, do které je potřeba na Incident zareagovat a začít s jeho řešením. Druhá hodnota poté označuje konečnou dobu, do které je potřeba Incident zcela vyřešit, tedy obnovit službu. Nedodržením těchto časových intervalů může dojít porušení smlouvy, což má za následek platbu pokuty. Dalším důležitým faktorem priority je reálný dopad na službu, tedy vážnost jednotlivých Incidentů. Pro příklad zde mohu uvést dva Incidenty – v prvním případě je server nedostupný, v druhém případě došlo k selhání zálohování. Zde je zcela zřejmé, že událost o nedostupnosti serveru je třeba řešit prioritně. Naopak zálohování lze vyřešit později, vzhledem k předem určeným časům pro automatickou tvorbu záloh.

Samotné řešení Incidentů probíhá na 3 úrovních, a to dle technických znalostí a zkušeností. První úroveň zastává Service desk (v případě zákaznických Incidentů) nebo Control desk (v případě monitorovacích Incidentů). Service desk převážně komunikuje se zákazníkem, případně zpracovává požadavky dle předem připravených postupů. Control desk provádí kontrolu stavu Incidentu, zda se např. nejedná o dočasný výpadek, nebo naopak se jedná o problém globálního charakteru. Poté provádí akce dle stanovených instrukcí a předává Incidenty dál na odpovědnou 2. úroveň. Smyslem Control desku je zamezit přetížení specialistů na 2. úrovni v situacích, kdy

nastanou větší problémy a je generováno velké množství Incidentů. Zároveň pomáhají s řešením Incidentů, pro které existuje dočasné řešení definované pomocí Problem Managementu.

Na 2. úrovni jsou zpracovávány složitější Incidenty, které vyžadují pokročilejší znalosti, případně vyšší úrovně oprávnění. Na 3. úrovni jsou poté nejzkušenější specialisti, kteří jsou odpovědní za konkrétní zákaznické prostředí a převážně pracují na zákaznických požadavcích, případně na tiketech týkajících se Problem a Change Managementu. Řešení Incidentu probíhá postupně od 1. úrovně, v případě výskytu reálného problému většinu Incidentů vyřeší až 2. úroveň. Specialista zde provádí analýzu Incidentu a bere do úvahy možné související předešlé Incidenty, případně probíhající Change nebo Problemy. [3, 8]

2.3.4 Problem Management

Zatímco Incident Management slouží k obnovení dodávané služby, Problem Management je využíván k řešení příčiny výpadku služeb. Jeho cílem je předcházet vzniku Incidentů takovým způsobem, abychom eliminovali opakující se Incidenty pomocí identifikace příčiny daného problému (hledáme tzv. root cause), pro který se snažíme implementovat permanentní řešení. Dalším cílem je minimalizovat dopad Incidentů, kterým nelze předcházet, nebo nemohou být permanentně vyřešeny, a to pomocí zdokumentovaných postupů s využitím tzv. workaround řešení. Proces dále dokumentuje vzniklé Problemy a jejich řešení, které je možné v případě potřeby zpětně dohledat a znovu použít. Ty se označují jako známe problémy (Known Error) a jsou uloženy v KEDB.

Problem převážně vzniká na základě jednoho nebo více předešlých Incidentů, u kterých nebyl nalezen zdroj problému nebo jej nebylo možné nadále řešit v rámci Incident Managementu, z důvodu potřeby hlubší investigace. Pomocí Problem Managementu můžeme také řešit tyto situace:

- Incidenty s velkým dopadem na službu (kritická priorita)
- Incidenty s dopadem na mnoho uživatelů
- Vícenásobný výskyt stejných Incidentů
- Incidenty, pro které neexistuje řešení
- Problémy globálního charakteru, které mohou ohrozit dodávané služby

Stejně jako u Incident Managementu, je pro Problem Management definované OLA, které smluvně definuje dobu pro nalezení příčiny Problemu a jeho vyřešení. V první fázi investigace Problemu je potřeba nalézt dočasné řešení, tzv. workaround. Ten zahrnuje instrukce pro první, případně druhou úroveň specialistů a umožňuje rychlejší řešení Incidentů. Zatímco Incident je obecně vyřešen v rámci hodin, Problem je řešen v rámci dní, někdy i týdnů. Proto je tento krok nezbytný.

Dále dochází k samotné investigaci problému, jeho analýze a identifikaci příčiny. Do úvahy je třeba také zahrnout nedávno proběhlé změny ve službě pomocí Change Managementu. Po nalezení příčiny se z něj stává známý problém (Known Error). Dalším krokem je hledání permanentního řešení. To v některých případech není možné aplikovat ihned, proto může dojít k přepracování workaround instrukcí, které budou využívány po dobu, než dojde na samotnou implementace opravy. Po aplikaci permanentního řešení nastává fáze validace, kdy se čeká na výsledky, zda řešení bylo úspěšné a daný Problem byl skutečně vyřešen. [4, 9]

2.3.5 Change Management

Change Management proces neboli proces řízení změn, se využívá k zajištění, aby všechny změny, ke kterým dochází v poskytované službě, byly korektně řízeny od jejich začátku až do konce, vždy řádně zaznamenány, analyzovány, naplánovány a schváleny, jejich implementace byla koordinována a na závěr přezkoumána. Účelem toho procesu je předcházet neočekávaným dopadům na samotnou službu a minimalizovat možná rizika při provádění změn. Jakýkoliv druh požadavku, jehož cílem je vytvořit, změnit nebo odstranit službu nebo servisní komponentu, by se měl řídit tímto procesem – např. změna softwaru, hardwaru, SLA aj.

Change se dělí na tři typy, které se liší podle situace využití. Change typu *Normal* je definovaná tímto procesem. Typ *Standard* se využívá pro předem definované (standardizované) úlohy, u kterých je dobře znám proces implementace a možná rizika. Díky tomu není ve většině případů vyžadováno schválení a dochází ke zjednodušení a urychlení procesu. Často se využívá předem připravených šablon. Posledním typem je *Emergency* Change. Ta se využívá v kritických situacích, kdy je vyžadováno okamžitého zásahu a je nepřípustná další časová prodleva, která by vznikla čekáním na schválení. Využívá se např. při bezpečnostních problémem nebo reálném ohrožení služby, např. při kritickém nedostatku místa na disku obsahující databázi.

První fází je tzv. design neboli vytvoření plánu. Ten se skládá z přesného popisu jednotlivých kroků, které mají být během implementace vykonány. Dále obsahuje analýzu rizik a možných problémů, které mohou nastat, dopad na samotnou službu, kroky, které je potřeba provést při testování, a také záložní plán pro případ selhání implementace, nebo nečekaných následků, způsobených implementací, aby bylo možné uvést službu zpět do původního (korektního) stavu. Důležité je také rozvrhnout časové servisní okno, které musí být předem domluveno se zodpovědnou osobou, případně se zákazníkem. Po vytvoření kompletního plánu je potřeba, aby Change byla schválena odpovědnou osobou. Zde může dojít na více situací, kdy Change může být zamítnuta a zrušena nebo pouze vrácena na přepracovaní, např. změna časového okna, nebo doplnění chybějících informací.

Následuje implementační fáze, kdy tzv. Change builder (osoba vykonávající Change) postupuje dle připraveného plánu a vykoná samotné změny. Poté nastává fáze testování, kdy jsou opět podle plánu provedeny kroky pro důkladné otestování výsledku implementace, případně dochází k sledování, zda se nevyskytují neočekávané problémy apod. Na závěr dochází k tzv. Post-Implementation Review fázi. Ta slouží ke zhodnocení celého průběhu implementace, ať po-

zitivnímu či negativnímu, a podání zpětné vazby pro možné budoucí zlepšení. V této fázi také Change zůstává po určitou dobu, pokud je očekáván výskyt nečekaných problémů. [5, 10]

2.4 Technická stránka

Po technické stránce byly vyžadovány znalosti o správě systému Windows. Během praxe jsem měl možnost seznámit se systémy od verze 2003, až po aktuální verzi 2012 R2. Dále jsem byl seznámen s principem monitoringu, jehož účelem je poskytovat informace o stavu serveru a jeho služeb. Významnou roli zde také hraje automatizace, která umožňuje specialistům snížit množství vynaložené práce pomocí předem připravených úloh.

2.4.1 Windows Server

Microsoft Windows Server je komerční operační systém určený jak pro malé, tak velké organizace. Jeho předností je široká škála nabízených služeb, které lze libovolně kombinovat a konfigurovat. Nejvýznamnější je adresářová služba Active Directory, která je založena na protokolu LDAP. Využívá se převážně k autentizaci uživatelů v doméně, řízení jejich přístupů a k centrálnímu ukládání informací o objektech v doméně. Navazuje na ni služba Group Policy, které umožňuje pomocí globálního nastavení definovat firemní politiky pro uživatele, stanice a servery, které patří do domény. To usnadňuje administrátorovi jejich konfiguraci.

Dále nabízí síťové služby, jako je DNS server pro překlad adres jak v interní, tak externí síti, a také DHCP server pro dynamickou správu přidělených IP adres. S rostoucím výpočetním výkonem se také rozšířilo využívání virtualizace, zde máme možnost využít služby Microsoft Hyper-V, která je ve specifických případech vhodnější, než konkurenční VMware vSphere. Často jsou také využívány webové služby IIS. Poslední službou bych jmenoval souborový server, který umožňuje síťový přístup k datům pomocí CIFS protokolu. Lze definovat pravidla pro přístup, kvóty pro jednotlivé uživatele i skupiny, filtrování pro určité typy souborů, tvorbu reportů a případně replikovat data na jiné servery. Windows Server samozřejmě nabízí i další služby, které jsem zde již neuvedl.

2.4.2 Monitoring

Pro zajištění kvality služeb je potřeba mít přehled o všech událostech, které se na serverech dějí. Aby bylo možné události efektivně zpracovávat, je potřeba využívat monitorovací nástroje. Během praxe jsem pracoval s nástroji BMC Patrol Central Operator, a Microsoft System Center Operations Manager. Oba nástroje pracují na podobném principu.

Na serveru je spuštěna klientská část aplikace. Ta obsahuje zásuvné moduly pro monitorování jednotlivých částí serveru. Může se jednat o modul pro monitorování operačního systému, monitorování hardwaru, MS SQL databází, využívání DHCP serveru a DNS služeb, stav Active Directory apod. Tyto moduly provádějí na základě nastaveného časového intervalu kontrolu

monitorovaných parametrů, kdy porovnávají jejich hodnoty vůči nastaveným varovným a kritickým hodnotám. V případě průniku jsou vyhodnoceny podmínky pro tvorbu Eventu. Tyto podmínky definují, zda se má Event vytvořit ihned nebo až po několika výskytech. Tímto se předchází tvorbě zbytečných Eventů (a Incidentů), vzniklých na základě dočasných problémů, které nemají vliv na chod služby. Hodnoty monitorovaných parametrů jsou uchovávány po stanovenou dobu, čehož se ve velké míře využívá při řešení Incidentů a Problemů. Díky tomu si může specialista zobrazit přehledně průběh parametru na časové ose a lépe pochopit povahu daného Incidentu.

2.4.3 Automatizace

Automatizační nástroje slouží k vykonání úloh, u kterých se očekává jejich pravidelné opakování, nebo je vyžadováno hromadné provedení na více serverech, a které je možné definovat pomocí sekvence kroků. To může zahrnovat instalaci servisních balíčků, upgrade systémových nástrojů a firmwaru, nebo získaní informací o serveru pro aktualizaci CMDB. Technické provedení je podobné jako u monitorovacích nástrojů. Na serveru běží klientská část aplikace, tzv. agent, která komunikuje s řídícím serverem. V operační konzoli poté volíme námi připravenou úlohu, které při jejím spuštění definujeme jeden nebo více serverů.

Princip úlohy je založen na automatizačním skriptu, který definuje jednotlivé příkazy, které jsou na daném serveru vykonány. Během praxe jsem se setkal s nástrojem BMC BladeLogic Server Automation. Jeho prostředí pro skriptování se nazývá NSH a je velice blízké prostředí Bash v Unixových systémech. Můžeme využívat jak možností tohoto prostředí, tak v případě potřeby spouštět další aplikace nebo skripty, v případě Windows např. PowerShell skripty, instalátory servisních balíčků a aplikací, provádět konfiguraci editací textových souborů nebo registrů, spouštět systémové příkazy aj.

Druhý způsob využití je vytvoření skriptů pro definované typy Incidentů a provést jejich částečné, nebo úplné vyřešení. V případě částečného řešení se může jednat o vytvoření diagnostického reportu, který již bude přiložen do tiketu a tím ušetřit specialistovi čas potřebný pro jeho vyřešení. V případě úplné automatizace se skript pokusí provést požadovanou opravu a vyřešit konkrétní problém.

3 Praktická část

Mým hlavním úkolem v týmu bylo zpracovávat automaticky generované Incidenty z monitorovacích nástrojů. Časová náročnost řešení jednotlivých Incidentů se lišila v závislosti na jejich typu a jednotlivých krocích řešení. V praxi se ve většině případů jednalo o jednotky až desítky minut pro vyřešení jednoho Incidentu. Menší problémy, které bylo možno vyřešit ihned, byly řešeny v rámci Incidentu, aby nedošlo k přetížení Problem Managementu. Poté následovalo pouze ověření, zda řešení bylo úspěšné. Každý den jsem obdržel nové Incidenty a ve většině případů je musel ještě téhož dne vyřešit.

3.1 Hardwarové Incidenty

Pro řešení hardwarových Incidentů bylo potřeba seznámit se s fyzickým řešením serverů, v tomto případě hlavně Blade řešením od společnosti Hewlett-Packard, jejich hardwarovou konfigurací, možnostmi vzdálené správy a s využíváním nástrojů pro kontrolu a diagnostiku hardwaru. Taktéž bylo nutné seznámit se s procesem výměny vadné součásti, pro který bylo nutno využít Change Management.

Celou výměnu bylo nutné důkladně naplánovat, analyzovat dopad na službu a vybrat nejvhodnější termín s ohledem na možné rizika při provozu s vadnou součástí. Následovalo kontaktování On-Site podpory společnosti Hewlett-Packard, které bylo potřeba dodat veškeré podklady o nutnosti výměny, dále se domluvit na čase výměny, a poté kooperovat s technikem, který prováděl samotnou výměnu v datacentru.

3.2 Systémové logy

Mezi velkou část Incidentů patří varovné zprávy ze systémového logu. Ty mohou být generované jak systémovými součástmi, tak jakoukoliv jinou službou nebo ovladačem. Pro řešení systémových zpráv bylo vhodné využívat portálu Microsoft TechNet, jenž slouží jako dokumentace pro jednotlivé ID událostí, popisuje jejich závažnost, možné příčiny a kroky pro jejich další diagnostiku a vyřešení. Při řešení těchto Incidentů bylo dobré také vždy zvážit, zda má daná událost význam pro chod služby a podniknout případné kroky pro úpravu monitorování, např. filtrováním pro dané CI, nebo globálně pro celého zákazníka.

3.3 Přetížení systémových prostředků

Dalším typem Incidentů bylo přetížení systémových prostředků, mezi které patřilo 100% využití procesoru po určitou dobu, vysoké využití stránkovacího souboru, příliš časté stránkování indikující nedostatek paměti, nedostatek místa na systémovém disku apod. Řešením těchto Incidentů bylo nalézt zdroj tohoto přetížení a provést nezbytné kroky k jeho odstranění. To mohlo v některých případech vést k zvětšení velikosti stránkovacího souboru, nebo ke změnám v hardwarové

konfiguraci serveru. Ve většině případů se však jednalo o problém s běžící službou nebo procesem. V tomto případě bylo potřeba zjistit její stav, analyzovat dopad na uživatele a případně službu restartovat nebo kontaktovat tým odpovědný za danou aplikaci.

V případě nedostatku místa na disku bylo potřeba provést analýzu adresářů, která zahrnovala nalezení dočasných souborů, které mohou být odstraněny, dále nalezení starých logů, které mohou být přesunuty nebo zkomprimovány, nalezení velkých aplikací, které nejsou součástí systému a je vyžadován jejich přesun na samostatný disk a odstranění záloh servisních balíčků a aktualizací. V případech, kdy nebylo možné uvolnit žádné, nebo jen malé množství místa, bylo nutné provést rozšíření disku pomocí Change Managementu. V případě virtuálních serverů se jednalo o jednoduchou záležitost, v případě fyzických serverů byla situace komplikovanější, vzhledem k nutnosti výměny hardwaru nebo přeuspořádání oddílů na disku.

3.4 Zálohování

Předposlední velkou skupinu tvořily Incidenty týkající se problémů se zálohováním. Zde nastávalo několik druhů problémů. Nejčastěji se vyskytovaly problémy se službou Windows Shadow Copy a tzv. writery, které slouží k zálohování souborů nebo dat, nad kterými probíhají operace, např. soubory databází, poštovních serverů aj. Účelem writeru je zálohovat soubor v konzistentním stavu, tedy po kompletním dokončení dané operace nad souborem a vyprázdněním bufferu. Writery se také využívají k zálohování systému. Zde mohlo dojít k selhání writeru, což vyžadovalo jeho opravu, počínaje restartováním služby až kompletním přeregistrováním v systému, případně opravou registrů.

Další problémy byly často síťového charakteru, kdy mohlo dojít k vyčerpání volných portů, změny cesty k zálohovacímu zařízení, změny názvu serveru, což mělo za následek odmítnutí zálohování na straně zálohovacího úložiště, případně chybějící otevřené porty, a to převážně na straně serveru. V některých případech se také jednalo o problémy se stabilitou připojení na straně zákazníka.

3.5 Ztráta konektivity

Mezi nejkritičtější Incidenty patří ztráta konektivity mezi monitorovaným a monitorovacím serverem. Ta může být způsobena následkem síťových problémů, neplánovaného restartování serveru, zastavením monitorovací služby na serveru, chybou na straně monitoringu, přetížením nebo zamrznutím serveru aj. Ačkoliv server může pracovat zcela v pořádku, ztráta konektivity způsobuje nefunkčnost celého monitorování. Ve všech případech je nutné ověřit, zda server je, či není dostupný přes monitorovací nástroj a podniknout další kroky pro zjištění, zda se jedná o problém na straně OS, sítě, nebo hardwaru a případně server uvést zpět do provozu.

3.6 Ostatní alarmy

Menší skupinou Incidentů byly problémy s neběžícími službami nebo procesy, které bylo nutné podle instrukcí uvést zpět do provozu, případně pomocí logů zjistit příčinu jejich nefunkčnosti a podniknout nezbytné kroky k jejich nápravě. Dále jsem se setkal s množstvím minoritních Incidentů, které bylo třeba řešit individuálně, např. nedostatečné práva pro monitorovacího klienta aj.

3.7 Automatizační tým

Na konci své praxe jsem se také stal členem nově vznikajícího automatizačního týmu, který má za úkol snížit množství vznikajících Incidentů, které nemají reálný dopad na službu nebo které je možné je vyřešit bez zásahu technika. V praxi se jedná o výběr nejčastěji vznikajících Incidentů, diskuzi o korektním nastavení monitorování a jejich vlivu na poskytovanou službu. Poté je průběh řešení těchto Incidentů specialisty zaznamenán do diagramu, který je použit pro vytvoření automatizačního skriptu. Zde je třeba zvážit veškeré možnosti, které mohou nastat, protože generovaný Incident bude ve většině případů řešen plně na straně automatizace a samotný tiket bude předán technikovi pouze při výskytu chyby v provádění skriptu. Je tedy vyžadováno, aby automatizace byla robustní a byla ošetřena vůči všem výjimkám. Pokud není možné Incident zcela automatizovat, je možné využít alespoň částečné cesty, kdy např. specialista obdrží tiket již se zpracovanou diagnostikou daného problému, což mu usnadní a hlavně urychlí výslednou práci potřebnou k obnovení služby.

3.8 Zhodnocení praxe

Během praxe jsem měl možnost rozšířit si své technické znalosti o operačním systému Windows a zásadách pro jeho správu. Zde jsem využil volitelného předmětu Správa Windows systémů, kde jsem získal základní přehled o systému, jeho službách, možnostech správy a celkový přehled nad touto platformou. Bohužel rozsáhlost tohoto systému není možné zahrnout do výuky jednoho semestru, proto jsem musel mnoho vědomostí potřebných k výkonu práce doplnit samostudiem. I přesto mi tento předmět velice pomohl, protože pan Ing. Návrat během svých přednášek zmiňoval mnoho běžných problémů z praxe, se kterými jsem se také setkal. Dále jsem využil znalostí z předmětu Počítačové sítě, konkrétně o TCP/IP modelu, které jsem využíval při řešení nejrůznějších síťových problémů na straně OS, ať už se jednalo o špatnou konfiguraci, problémy s firewallem nebo diagnostiku ostatních příčin problémů s komunikací.

Během praxe jsem musel mnoho svých znalostí doplnit samostudiem. Převážně jsem čerpal z interně připravených dokumentů s řešením v praxi nejčastěji vyskytujících se problémů. Často jsem ale také využíval technickou dokumentaci od výrobců softwaru, v případě hardwaru od společnosti Hewlett-Packard a dále online databáze odpovědí jako jsou Microsoft TechNet nebo IBM Knowledge Center. Mezi nejvýrazněji chybějící znalosti bych však uvedl neznalost ITIL procesů, kterých bylo nutné se držet od začátku praxe. Jako další chybějící znalosti v době

nástupu bych uvedl malou znalost serverových technologií, monitorovacích a automatizačních nástrojů a hlubší znalost Active Directory.

Tato praxe mi však umožnila tyto nedostatky odstranit a získat přehled v serverových technologiích, nejen z pohledu OS, ale také celkového řešení infrastruktury, hardwarových možnostech Blade serverů, řešení síťového uložení dat (SAN) nebo možnostech virtualizace jako je Microsoft Hyper-V nebo VMware vSphere. Velice zajímavé bylo také školení o principu clusteringu, kde jsem pochopil zásady pro zajištění maximální dostupnosti služby i v případě výpadku serveru.

4 Závěr

Možnost absolvovat odbornou praxi na této pozici byla pro mě velice přínosnou zkušeností, díky niž jsem si rozšířil nejen své technické vědomosti, ale také pochopil velice potřebnou procesní stránku, o které jsem se dozvěděl až při svém nástupu na praxi. Zároveň jsem měl možnost pracovat v nadnárodní společnosti a vyzkoušet si práci v týmu, kdy je potřeba dobré organizace a rozdělení práce mezi méně zkušené a více zkušené specialisty, vzájemná spolupráce při řešení rozsáhlejších problémů, sdílení zkušeností, odpovědnost za přidělenou práci a potřeba správného rozhodování se v kritických situacích. Praxi hodnotím velice pozitivně a věřím, že vědomosti získané během ní mi budou i v budoucnu přínosem.

Literatura

[1] Historie. *Tieto - IT, výzkum a vývoj a poradenství.* [online]. [cit. 2016-04-22]. Dostupné z: `https://www.tieto.cz/tieto-o-nas/historie-tieto-czech-republic`

[2] Informace o Tieto. *Tieto - IT, výzkum a vývoj a poradenství.* [online]. [cit. 2016-04-22]. Dostupné z: `https://www.tieto.cz/tieto-o-nas`

[3] ITIL Incident Management: Best Practices & Process Flow. *BMC - Bring IT to Life with Digital Enterprise Management* [online]. [cit. 2016-04-14]. Dostupné z: `http://www.bmc.com/guides/itil-incident-management.html`

[4] ITIL Problem Management: Best Practices & Processes Flow. *BMC - Bring IT to Life with Digital Enterprise Management* [online]. [cit. 2016-04-16]. Dostupné z: `http://www.bmc.com/guides/itil-problem-management.html`

[5] ITIL Change Management: Best Practices & Processes. *BMC - Bring IT to Life with Digital Enterprise Management* [online]. [cit. 2016-04-19]. Dostupné z: `http://www.bmc.com/guides/itil-change-management.html`

[6] TietoWay - Configuration management. *TietoWay* [online]. [cit. 2016-04-15]. Dostupné z: `http://tway.intra.tieto.com/processes/195/530/534/795`

[7] TietoWay - Event management. *TietoWay* [online]. [cit. 2016-04-15]. Dostupné z: `http://tway.intra.tieto.com/processes/195/530/614`

[8] TietoWay - Incident management. *TietoWay* [online]. [cit. 2016-04-14]. Dostupné z: `http://tway.intra.tieto.com/processes/195/530/537`

[9] TietoWay - Problem management. *TietoWay* [online]. [cit. 2016-04-16]. Dostupné z: `http://tway.intra.tieto.com/processes/195/530/631`

[10] TietoWay - Change management. *TietoWay* [online]. [cit. 2016-04-19]. Dostupné z: `http://tway.intra.tieto.com/processes/195/530/565`